REMARKS

The above Amendments and these Remarks are in reply to the Office Action mailed July 14, 2004

Currently, claims 1-60 are pending. Applicants have amended claims 1, 7, 13, 27, 36, 39, 43, 46, 50, and 56, cancelled claims 53-55, and added claims 61-63. Applicants respectfully request reconsideration of claims 1-52 and 56-60 and consideration of newly added claims 61-63.

I. Information Disclosure Statement Filed March 8, 2004

An information disclosure statement (IDS) was filed on August 23, 2002. The copy of the Office Action received by Applicants only includes a copy of page 1 of the IDS bearing the Examiner's initials to indicate consideration of the cited references. However, the IDS included two pages. The second page disclosed the reference: Park et al., "Secure Cookies on the Web," IEEE Internet Computing, July/August 2000. The Examiner is respectfully requested to initialize the reference disclosed on page 2 of the IDS to indicate consideration thereof and to provide Applicants with a copy of the initialized form (all pages) with the next action from the USPTO. A copy of the IDS is included with this response for the Examiner's convenience. If the USPTO has misplaced the copy of the submitted reference, the Examiner is asked to please contact the undersigned so that a duplicate copy can be furnished for consideration.

II. Objection to the Specification

Applicants' Specification includes text in the form of hyperlinks to explain the use of universal resource locators (URL) in accordance with embodiments of the invention. As the MPEP states, where "the hyperlinks themselves, rather than the contents to which the hyperlinks are directed, are part of applicant's invention and it is necessary to have them included in the patent application in order to comply with the requirements of 35 U.S.C. 112, first paragraph, and applicant does not intend to have these hyperlinks be active links, examiners should not object to these hyperlinks. *MPEP § 608.01.* Applicants assert that the hyperlinks in the specification themselves, rather than the contents to which they are directed, are part of Applicants' invention and are not intended to be active links. Accordingly, Applicants respectfully request withdrawal of the objection to the Specification under *MPEP § 608.01.*

III. Rejections under 35 U.S.C. § 102(e)

Claims 1, 2, 6, 7, 9-22, 26, 27, 31-36, 39-43, 46-50, 53, 56, 59, and 60 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,226,752 ("*Gupta*"). Because *Gupta* fails to disclose each limitation of claims 1, 2, 6, 7, 9-22, 26, 27, 31-36, 39-43, 46-50, 53, 56, 59, and 60 after entry of the present amendments, Applicants assert that these claims are patentable over the cited art.

Overview of Invention

Embodiments of Applicants' invention provide an "application program interface for an access system that enables an application without a web agent front end to use contents of an existing cookie (or other storage mechanism) to provide access system services." *Applicants' Specification*, p. 4, ll. 4-7 (*emphasis added*). A key component of Applicants' invention is the application program interface (API) which allows applications to access the authorization services of an Access System. For example, an application on an application server "can access many of the authentication and authorization services" from the Access System by using the Access System API. *Id.* at p. 90, ll. 11-15. The application can directly determine authorization of a user for a resource using the API into the Access System without re-routing users and clients to the Access System.

Claims 1, 2, 6, 7, 9-22, 26, 36, 39-42, 43, 46-49

Independent claims 1, 36, and 43 have been amended to capture the concept of the Application Program Interface for an Access System and now recite:

> receiving user session state information for a first user at an application program interface for an access system, said user session state information is from an application without a web agent front end. (*Emphasis added*).

In amended claims 1, 36, and 43, user state information is received at the application program interface from an application without a web agent. Because *Gupta* does not disclose an application program interface for an access system as recited in amended claims 1, 36, and 43,

Gupta cannot anticipate claims 1, 36, and 43. In *Gupta*, there is no application program interface. For example, Figure 2 of *Gupta* to which the cited teachings pertain merely shows three players in the disclosed system – a client, an application server, and a login server. *See Gupta*, Figure 2, col. 11 – col. 12. Nowhere does *Gupta* mention or disclose an application program interface for an access system or for a login server as disclosed therein. Because *Gupta* fails to disclose an application program interface for an access system, *Gupta* does not disclose the receipt of "user state information for a first user at an application program interface for an access system," and cannot anticipate claims 1, 36, and 43.

Moreover, in the cited teachings of *Gupta*, *Gupta* teaches that if there is no valid session, "the application server redirects the client's request to a login server." *Id.* at col. 12, ll. 14-17. Accordingly, *Gupta* does not teach that an application provides user state information to an application program interface for an access system. Rather, *Gupta* teaches that the application server redirects the client's request to the login server. As recited in claim 1, there is no redirection of a client to the access system. Rather, the authorization services of the access system are provided to the application via the application program interface by receiving from the application "user state information for a first user at an application program interface."

To capture the idea that the authorization services of an access system are provided to an application via an application program interface for the access system, claims 1, 36, and 43 have also been amended to recite:

> providing authorization services of said access system to said application using said application program interface in an attempt to authorize said first user to access said first resource without requiring said first user to re-submit authentication credentials.

Gupta does not disclose any means for providing authorization services of an access system to an application using an application program interface. In that portion of *Gupta* cited for teaching the previously recited "attempting to authorize" step, *Gupta* teaches that after a successful authentication at the login server, the login server redirects the browser back to the application server and can transmit a cookie or token for the login server to the client's browser. *Gupta*, col. 12, ll. 47-54. *Gupta* further teaches that:

> "[b]y storing the cookie, the login server can easily determine if the client has been previously authenticated (e.g., by

> retrieving the cookie or token) and may not require the user to reenter necessary information (e.g., a username and password). *Id.* at ll. 54-58.

While *Gupta* teaches that the login server can use a cookie to determine if a client has been previously authenticated, *Gupta* does not disclose any means or technique for "providing authorization services to said application using said application program interface," as recited in claims 1, 36, and 43. In *Gupta*, the cookie is simply used by the login server to avoid having the user "reenter necessary information (e.g., a username and password)." *Id.* If authentication is necessary, *Gupta* teaches redirection of a client to the login server for authentication. Thus, *Gupta* simply discloses that a login sever checks for a cookie to avoid user resubmission of authentication credentials. At not point does *Gupta* mention an application program interface or the use of an application program interface to directly provide authorization services to an application. Accordingly, *Gupta* fails to disclose "providing authorization services of said access system to said application using said application program interface," as recited in claims 1, 36, and 43 (*emphasis added*).

Because *Gupta* fails to disclose each of the limitations of claims, 1, 36, and 43, Applicants assert that these claims are patentable over the cited art. Claims 2, 6, 7, 9-22, 26, 27, 31-35, 39-42, 46-50, 53, 56, 59, and 60 each ultimately depend from one of claims 1, 36, or 43 and therefore, should be patentable for at least the same reasons.

Claims 27, 31-35, 50

Independent claims 27 and 50 have also been amended to recite an "application program interface for an access system" and related functionality performed by the application program interface. For example, claims 27 and 50 each recite:

> providing said information from said cookie to an application program interface for an access system.

In *Gupta*, there is no application program interface, and information from a cookie is not provided to such an interface. As cited, *Gupta* teaches that the "application server redirects the client's request to a login server" by sending a "redirect message (with the login server's URL) back to the client's browser." *Gupta*, col. 12, ll. 13-16. While *Gupta* discloses that the redirect message may include a cookie for the application, the redirect message (including the cookie) is

provided to the user's browser, not to "an application program interface for an access system," as recited in claims 27 and 50.

Claims 27 and 50 have further been amended to recite:

> with said application, accessing authorization services of said access system using said application program interface, said accessing includes requesting said access system interface to authorize said first user to access said first resource based on information from said electronic request from said first user and based on said information from said cookie.

In the cited portions of *Gupta*, authentication of a user is performed by redirecting the user's browser to the login server. *Gupta* teaches that a cookie may be transmitted to the client's browser so that the "login server can easily determine if the client has been previously authenticated" *Gupta*, col. 12, ll. 54-58. However, the login server still determines if the client has been previously authenticated. Nowhere does *Gupta* mention the use of an application program interface for an access system as recited in claims 27 and 50.

Moreover, *Gupta* discloses no means or technique for accessing authorization services "with said application," as recited in claims 27 and 50. *Gupta* teaches redirection of a user to the login server for authentication if authentication is necessary. There is no mention of techniques or means for allowing an application to access "authorization services of said access system using said application program interface," as recited in claims 27 and 50. Redirecting a user to a login server for authentication is substantially different and distinct from using an application to directly access "authorization services of said access system using said application program interface," as recited in claims 27 and 50.

Because *Gupta* fails to disclose each of the limitations of claims 27 and 50, Applicants assert that these claims are patentable over the cited art. Claims 31-35 each ultimately depend from claim 27 and therefore, should be patentable for at least the same reasons.

Claims 56, 59, and 60

Amended independent claim 56 recites:

> authenticating a first user;
> causing user session state information to be stored at a client for said first user;
> authorizing said first user to access a first protected

resource;

receiving a request from an application without a web agent front end to allow said first user to access a second protected resource, said step of receiving a request includes receiving said user session state information from said application; and

authorizing said first user to access said second protected resource without requiring said first user to re-submit authentication credentials, if said first user is authorized to access said second protected resource.

As recited in the method of claim 1, a user is authenticated and user state information stored at a client for that user. The method then recites "authorizing said first user to access said second protected resource without requiring said first user to re-submit authentication credentials." *Gupta* does not disclose authorizing a first user to access a "second protected resource without requiring said first user to re-submit authentication credentials." In the cited portion of *Gupta* at col. 12, ll. 41-61, *Gupta* deals with the authentication of a user, not with the authorization of user. Authentication and authorization are not the same. For example, an authenticated user may not be authorized to access a particular resource.

Gupta teaches that after a login server successfully authenticates a user, the login server "redirects the browser back to the application server along with the session information." *Gupta*, col. 12, ll. 47-49. *Gupta* further teaches that a cookie (or token) for the login server may be transmitted to the client's browser. "By storing the cookie, the login server can easily determine if the client has been previously authenticated (e.g., by retrieving the cookie or token) and may not require the user to reenter necessary information (e.g., a username and password)." *Id.* at ll. 54-58 (*emphasis added*).

Gupta's cited teachings with respect to cookies in this regard are directed to authentication. *Gupta* is teaching that the login server can determine from a cookie stored on a client that the client has been previously authenticated. *Gupta* later discusses authorization but does address the use of a cookie to authorize the user for a second resource. *Gupta* is explaining the use of cookies to avoid having a user resubmit information if that user has been previously authenticated. Accordingly, *Gupta* does not disclose "authorizing said first user to access said second protected resource without requiring said first user to re-submit authentication credentials,

if said first user is authorized to access said second protected resource," as recited in claim 56 (*emphasis added*).

Because *Gupta* fails to disclose each of the limitations of claim 56, Applicants assert that claim 56 is patentable over the cited art. Claims 59 and 60 each ultimately depend from claim 50 and should be patentable for at least the same reasons.

IV. Rejection of Claims 3-5, 8, 28-30, 37, 38, 44, 45, 51, 52, 54, 55, 57, and 58

Claims 3-5, 8, 28-30, 37, 38, 44, 45, 51, 52, 54, 55, 57, and 58 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Gupta* in view of U.S. Patent No. 6,668,322 ("*Wood*"). Because the proposed combination of *Gupta* and *Wood* fails to teach or suggest each of the limitations of claims 3-5, 8, 28-30, 37, 38, 44, 45, 51, 52, 54, 55, 57, and 58, Applicants assert that these claims are patentable over the cited art.

As set forth above, *Gupta* fails to disclose "an application program interface for an access system," as recited in amended independent claims 1, 27, 36, 43, and 50, It is further submitted that *Gupta* fails to suggest such a limitation. *Gupta's* cited teachings do not mention an application program interface for an access system at all. Instead, *Gupta's* teaches redirecting users to a login server for authentication. Accordingly, *Gupta* fails to teach or suggest the use of an "application program interface for an access system," as recited in claims 1, 27, 36, 43 and 50. *Wood* has been cited for the disclosure of limitations of various claims dependent from one of claims 1, 27, 36, 43, or 50. Because *Gupta* fails to teach or suggest the limitations for which it is cited, the combination formed by the addition of *Wood's* cited teachings also fails to teach or suggest each of the limitations of claims 1, 27, 36, 43, and 50. Because the proposed combination of *Gupta* and *Wood* fails to teach or suggest each of the limitations of claims 1, 27, 36, 43, and 50, Applicants assert that these claims are patentable over the cited art. Claims 3-5, 8, 28-30, 37, 38, 44, 45, 51, 52, 54, and 55 each ultimately depend from one of claims 1, 27, 36, 43, and 50 and should be patentable for at least the same reasons.

As also set forth above, *Gupta* fails to disclose "authorizing said first user to access said second protected resource without requiring said first user to re-submit authentication credentials, if said first user is authorized to access said second protected resource," as recited in amended independent claim 56. It is further submitted that *Gupta* fails to suggest such a limitation. *Gupta's* cited teachings are limited to the use of cookie to avoid having a previously

authenticated user resubmit necessary information. *Gupta's* teachings are not directed to the use of such a cookie for authorizing a user for a second resource as recited in claim 56. Accordingly, *Gupta* fails to teach or suggest "authorizing said first user to access said second protected resource without requiring said first user to re-submit authentication credentials, if said first user is authorized to access said second protected resource," as recited in claim 56. Because *Gupta* fails to teach or suggest the limitations for which it was cited, the combination formed by the addition of *Wood's* cited teachings also fails to teach or suggest each the limitations of claim 56. Because the proposed combination of *Gupta* and *Wood* fails to teach or suggest each of the limitations of claim 56, Applicants assert that claim 56 is patentable over the cited art. Claims 57 and 58 each ultimately depend from claim 56 and should be patentable for at least the same reasons.

V. Rejection of Claims 23-25

Claims 23-25 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Gupta* in view of U.S. Patent No. 6,286,098 ("*Wenig*"). As set forth above, *Gupta* fails to teach or suggest each of the limitations of claim 1. Because *Gupta* fails to teach or suggest the limitations for which it is cited, the combination formed by the addition of *Wenig's* cited teachings also fails to teach or suggest each of the limitations of claim 1. Because the proposed combination of *Gupta* and *Wenig* fails to teach or suggest each of the limitations of claim 1, Applicants assert that claim 1 is patentable over the cited art. Claim 23-25 each ultimately depend from claim 1 and should be patentable for at least the same reasons.

VI. Newly Added Claims

Claims 61-63 have been added. Applicants respectfully submit that the newly added claims are patentable over the cited art. Independent claim 61 recites a system that includes four elements: a client; at least one application; an access server; and an application program interface for said access server. *Gupta* fails to disclose or suggest such a combination of elements. As previously described, *Gupta* includes three elements (Figure 2): a client; an application server; and a login server. *Gupta* does not mention the use of a an application program interface for an access server or for the login server disclosed therein. Moreover, in claim 61, the application program interface provides "authorization services to said at least one application." *Gupta* does

not suggest such a configuration. In *Gupta*, the application server redirects a user to the login server for authentication. There is nothing to suggest an application program interface that can provide authorization services to an application. Because the prior art fails to teach or suggest each of the limitations of claim 61, Applicants assert that claim 61 (and by their dependency, claims 62 and 63) is patentable over the cited art.

VII. Conclusion

Based on the above amendments and these remarks, reconsideration of claims 1-52 and 56-60, and consideration of newly added claims 61-63 is respectfully requested.

The Examiner's prompt attention to this matter is greatly appreciated. Should further questions remain, the Examiner is invited to contact the undersigned attorney by telephone.

Enclosed is a PETITION FOR EXTENSION OF TIME UNDER 37 C.F.R. § 1.136 for extending the time to respond up to and including November 14, 2004.

The Commissioner is authorized to charge any underpayment or credit any overpayment to Deposit Account No. 501826 for any matter in connection with this response, including any fee for extension of time, which may be required.

Respectfully submitted,

Date: October 19, 2004

By: _____
David E. Cromer
Reg. No. 54,768

VIERRA MAGEN MARCUS HARMON & DENIRO LLP
685 Market Street, Suite 540
San Francisco, California 94105-4206
Telephone: (415) 369-9660
Facsimile: (415) 369-9665